Brody Valerga (11789)
Valerga LLP
395 S. Main Street #201
Alpine, UT 84004
(801) 893-3635
brody@valergalawyers.com

Paul J. Doolittle, Esq.*
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com
Attorneys for Plaintiff
**Pro Hac Vice forthcoming*

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

SIERRA VENT, individually and on behalf of all others similarly situated, ***Plaintiff*,** **v.** **HEALTHEQUITY, INC.,** ***Defendant.***	**COMPLAINT** **JURY TRIAL DEMANDED** Case No.: 2:24-cv-00685-RJS Judge Robert J. Shelby

CLASS ACTION COMPLAINT

Plaintiff Sierra Vent, ("Plaintiff") brings this Class Action Complaint against Defendant, HealthEquity Inc., ("Defendant") as an individual and on behalf of all others similarly situated,

and alleges, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

SUMMARY OF ACTION

Plaintiff brings this action against Defendant because its privacy practices leave consumers' data vulnerable to hacking and theft. The unauthorized disclosure of Plaintiff's personally identifiable information constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's failure to adequately secure the personal data in its custody, and has resulted in actual, particularized, and concrete harm to the Plaintiff. The invasion of Plaintiff's privacy, and resulting loss of control over her confidential information, is an actual injury. Furthermore, Defendant has made material misrepresentations in its privacy policy regarding its privacy and security requirements for its subcontractors. Defendant's failure to adhere to the steps, standards, and promises contained in its privacy policy has resulted in harm to the Plaintiff. Therefore, Plaintiff brings this action to recover damages, in an amount to be determined at trial, attorneys' fees, and costs. Plaintiff is also seeking injunctive relief requiring Defendant to: (i) regularly assess the risks to its entire attack surface and confirm that its administrative, technical, and physical safeguards are appropriate to protect the confidential information in its custody; (ii) continuously monitor its vendors, at least once per year, to identify potential ways a threat actor could gain access to confidential information; (iii) implement an administrative process for regularly auditing its subcontractors' privacy and security standards, including, adherence to a Zero Trust model of strict access controls to reduce the possibility of unauthorized disclosures; and (iv) comply with the HIPAA Privacy, Security and Breach Notice Rules. Plaintiff respectfully requests the Court to hold Defendant responsible for its conduct in contributing to this data breach.

STATEMENT OF FACTS

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the protected health information ("PHI") and other personally identifiable information ("PII") that it stored in an unstructured data repository outside its core systems, including, but not limited to: first name, last name, address, telephone number, employee ID, employer, social security number, health card number, health plan member number, dependent information, service type, diagnoses, prescription details, and payment card information.

2. Defendant is the custodian of Health Savings Accounts ("HSA") and a directed third-party administrator of COBRA plans associated with BlueCross Blue Shield of South Carolina. In its role as a third-party administrator of a health plan, Defendant collects, creates, or shares information about health status, the provision of health care, or payment for health care that can be used to identify an individual.

3. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Defendant is considered a business associate. As a business associate, Defendant is obligated to safeguard sensitive information, even when stored in an unstructured format. Unfortunately, Defendant failed to meet its obligations to protect the sensitive information in its custody or under its control.

4. On, or about, March 25, 2024, Defendant detected unauthorized activity within a third-party cloud environment and determined that a business partner—with access to the cloud storage environment—had their account credentials compromised, which permitted an unauthorized party access to Plaintiff's personal information (hereafter referred to as the "Data

Breach"). Furthermore, some of the PHI/PII accessed in the Data Breach was subsequently transferred from the business partner's network to another unidentified, unauthorized third-party.[1]

5. Defendant is required to comply with the HIPAA Privacy Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 expanded the responsibilities of business associates under the Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

6. The HIPAA Privacy Rule and Security Rule establishes standards for the protection of protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a covered entity. *See* 45 C.F.R. § 160.103.

7. The Privacy Rule requires Defendant to implement appropriate safeguards to protect the privacy of protected health information. The Security Rule requires Defendant to implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The Security Rule defines "confidentiality" to mean that e-PHI is not available or disclosed to unauthorized persons. The HIPAA rules also require Defendant to provide notice of an unauthorized disclosure of unencrypted protected health information, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

[1] *See,* HealthEquity, Inc., Form 8-K, July 2, 2024, available here: https://www.sec.gov/ix?doc=/Archives/edgar/data/1428336/000142833624000055/hqy-20240702.htm

8. Under HIPAA, Defendant also had a duty to assess the security practices of its "business partners" to ensure that they are adequately securing any PHI to which they have access. Without conducting a risk analysis of its "business partners," it is impossible to identify the appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Plaintiff's PHI/PII.

9. Upon information and belief, the Data Breach occurred because Defendant failed to regularly review its records to track access to Plaintiff's PHI/PII, failed to periodically evaluate the effectiveness of its security measures regarding information access management, and/or failed to regularly reevaluate the potential risks to the PHI/PII stored in cloud environments.

10. Defendant further had a duty to ensure that any "business partners" with access to PHI/PII agree to be bound by the same restrictions, conditions, and requirements that apply to Defendant with respect to such information.

11. Defendant's published privacy policy provides, in part, "HealthEquity places a high priority on protecting your personal information. We maintain administrative, technical, and physical safeguards designed to protect the information that you provide on this website and in connection with the Services from unauthorized access to or acquisition of such information. . . . [HealthEquity will ***require***] ***our subcontractors to maintain the same privacy and security standards for protecting your information as we do***."[2]

12. Under its "Security & IT" webpage, Defendant represents that "[a]s part of our remarkable service, we are committed to protecting the confidentiality, integrity, and availability of your personal information and our systems and applications. This site explains our approach to

[2] *See*, HealthEquity General Privacy Notice, *Information Security*, available here: https://www.healthequity.com/privacy/general

securing your data against cyber threats…"[3] One of Defendant's "Guiding Principles" is the adoption of the Zero Trust security framework. The Zero Trust framework is a security concept premised on "never trust, always verify." Two of the main principles of the Zero Trust framework are:

a. **Verification**—always authenticate and authorize based on all available data points, including user identity, location, and device; and

b. **Least-Privilege Access**—user access should be limited with just-in-time (JIT) and just-enough access (JEA) risk-based adaptive policies.

13. A Zero Trust model requires strict access controls to reduce the possibility of unauthorized access and data breaches. A key component of the Zero Trust framework is multi-factor authentication (MFA), which requires multiple forms of verification before granting access to resources, such as cloud storage. In the Zero Trust model, trust is never assumed, and every access request is treated as if it originated from an untrusted network. MFA reduces the risk of data breaches by requiring more than just a username and password—a security token or biometric factor—to access resources.

14. Upon information and belief, the Data Breach occurred because Defendant failed to ensure that its "business partners" or subcontractors with access to PHI/PII maintained the same privacy and security standards as Defendant. More specifically, Defendant failed to ensure that its business partners/subcontractors adopted the Zero Trust model of network security and implemented multi-factor authentication and other access management policies regarding the PHI/PII stored in cloud environments.

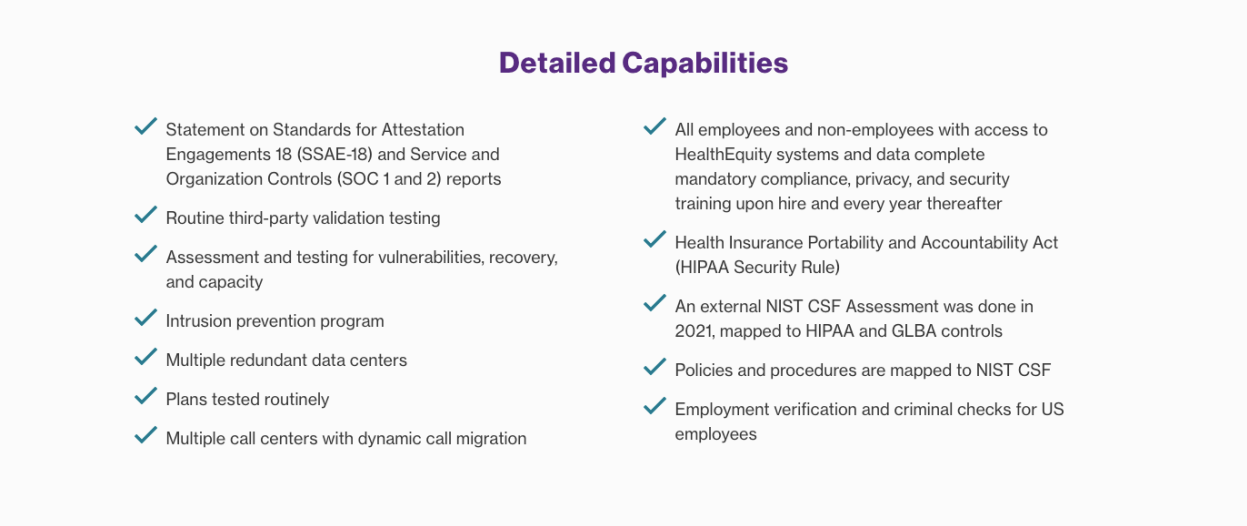
[3] *See*, HealthEquity General Privacy Notice, *Security & IT*, available here: https://www.healthequity.com/security

15. Under HIPAA's Breach Notice Rule, Defendant had a duty to notify affected individuals following the discovery of the Data Breach. Breach notice must be provided without unreasonable delay and in no case later than 60 days following the discovery of the breach.

16. On or about August 23, 2024, Defendant mailed data breach notice letters to individuals who were affected by the data breach. Omitted from the data breach notice letter were the details of the root cause of the "system anomaly" discovered on March 25, 2024, how the vendor's user credentials were compromised, and the remedial measures undertaken to ensure this type of data breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff, who retains a vested interest in ensuring that her PHI/PII remains protected.

17. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's data was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the information from those risks left the data in a dangerous condition.

18. Alternatively, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's data was a risk that Defendant should have known because Defendant touts its policies and procedures are mapped to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).



*Screenshot of HealthEquity Security & IT capabilities

19. The NIST CSF embodies five (5) core functions: (a) Identify; (b) Protect; (c) Detect; (d) Respond; and (e) Recover. The "detect" function required Defendant to detect potential attack vectors through continuous monitoring of the entire attack surface.[4] A data breach through a third-party vendor is possible when vendors require access to sensitive data to perform their duties. Since many cyberattacks target third-party vendors, under NIST CSF, Defendant should have been continuously monitoring its business partner/service provider attack surface to identify potential ways a hacker could gain access to PHI/PII or other confidential information.

20. Upon information and belief, the Data Breach occurred because Defendant failed to adhere to its policies and procedures that were mapped to the NIST CSF. More specifically, Defendant failed to continuously monitor its vendors' security practices and/or continuously monitor its vendors for data exposures and compromised credentials. The use of data leak detection software (or requiring vendors to implement data leak detection software) would have detected compromised credentials and prevented the Data Breach.

[4] An attack vector is a method of gaining unauthorized access to a network or computer system. An attack surface is the total number of attack vectors a threat actor can use to access and exfiltrate data.

21. The Data Breach was a direct result of Defendant's failure to implement reasonable safeguards to protect PHI/PII from a foreseeable and preventable risk of unauthorized disclosure. Had Defendant implemented administrative, technical, and physical controls consistent with its privacy policy, industry standards and best practices, it could have prevented the Data Breach.

22. Defendant's conduct resulted in the unauthorized disclosure of Plaintiff's private information to cybercriminals, which a reasonable person would find offensive. The unauthorized disclosure of Plaintiff's PHI/PII constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's failure to adequately secure the PHI/PII in its custody, and has resulted in actual, particularized, and concrete harm to the Plaintiff. The invasion of Plaintiff's privacy is an actual injury that does not require economic or special damages; Plaintiff sustained general damages such as the loss of the right to control one's own information, embarrassment, and diminution in the value of the PHI/PII that was compromised in the Data Breach. The injuries Plaintiff suffered, as described herein, can be redressed by a favorable decision in this matter.

23. Defendant has not provided any assurances that: all data acquired in the Data Breach, or copies thereof, have been recovered or destroyed; or, that Defendant has modified its data protection policies, procedures, and practices sufficient to avoid future, similar, data breaches.

24. "Data breaches in healthcare have reached alarming levels, with the Office of Civil Rights reporting 725 notifications of breaches in 2023, where more than 133 million records were exposed or impermissibly disclosed."[5] Plaintiff faces a substantial risk of future medical identity theft or fraud where Plaintiff's unique medical identifying information was obtained by cybercriminals in a targeted attack. Medical identity theft involves the misuse of a person's unique

[5] *Healthcare fraud and the burden of medical ID theft*, available at: https://www.experian.com/blogs/healthcare/healthcare-fraud-and-the-burden-of-medical-id-theft/

medical identity to wrongfully obtain health care goods, services, or funds.[6] Medical identity theft "can result in bills for procedures the patient has never had, inaccurate medical records, and potentially life-threatening care."[7]

25. Typically, hackers sell the PHI/PII "to criminals who create phony providers to submit fraudulent claims on a mass scale that can result in hundreds of millions of dollars in Medicaid, Medicare, or other insurance fraud."[8]

26. Defendant's conduct, as evidenced by the circumstances of the Data Breach, has created a substantial risk of future identity theft, fraud, or other forms of exploitation. The circumstances demonstrating a substantial risk of future exploitation include, but are not limited to:

a) **Sensitive Data Type**: The data acquired in the Data Breach included unencrypted social security numbers, health card numbers, health plan member numbers, diagnoses, prescription details, and payment card information. Upon information and belief, this category of data is used by cybercriminals to perpetuate fraud, identity theft, and other forms of exploitation.[9]

b) **Data Breach Type**: Defendant detected unauthorized activity within a third-party cloud environment on March 25, 2024. Three months later, on June 26, 2024, Defendant determined that a business partner—with access to the cloud storage environment—had their account credentials compromised. Upon information and belief, other business partners had their credentials compromised, which creates a substantial risk of future exploitation attempts.

c) **Data Misuse**: The Data Breach may have exposed the PHI/PII of 4,300,000 people.[10] Some of the PHI/PII accessed in the Data Breach was subsequently transferred to another unidentified, unauthorized third-party.[11] Cybercriminals, upon information and belief, generally sell stolen PHI/PII on the dark web or

---

[6] *See*, *Common Types of Health Care Fraud*, Center for Medicare & Medicaid Services (CMS) Fact Sheet, available at: https://www.cms.gov/files/document/overviewfwacommonfraudtypesfactsheet072616pdf

[7] *Healthcare fraud and the burden of medical ID theft*, available at: https://www.experian.com/blogs/healthcare/healthcare-fraud-and-the-burden-of-medical-id-theft/

[8] *Someone could steal your medical records and bill you for their care.* https://www.npr.org/sections/health-shots/2023/07/26/1189831369/medical-identity-fraud-protect-yourself

[9] https://www.f-secure.com/us-en/articles/why-do-hackers-want-your-personal-information

[10] *See,* Data Breach Notifications, Office of the Maine Attorney General, available here: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2ec3e314-5731-49d0-a937-6dc22c6b24f3.html

[11] *See*, FN1, *supra.*

> post it for free on the internet. The dark web uses a series of encrypted networks to hide users' identities, which makes it convenient for criminals to buy and sell illegally obtained data. Many criminals purchase stolen personal data off the dark web before launching social engineering-based attacks. A social engineering attack is a method of using psychological manipulation to deceive a victim and gain access to a computer system or to steal sensitive information such as login credentials. Social engineering attacks that can be launched using names, telephone numbers and email addresses include phishing, smishing (SMS message), vishing (voice messaging), pretexting, and baiting attacks.

27. The imminent risk of future harm resulting from the Data Breach is traceable to the Defendant's failure to adequately secure the PHI/PII in its custody, and has created a separate, particularized, and concrete harm to the Plaintiff.

28. More specifically, the Plaintiff's exposure to the substantial risk of future exploitation caused them to: (i) spend money on mitigation measures like credit monitoring services and/or dark web searches; (ii) lose time and effort spent responding to the Data Breach; (iii) experience emotional distress (frustration, fear, embarrassment, and anger) associated with reviewing accounts for fraud, changing usernames and passwords or closing accounts to prevent fraud; and, (iv) general anxiety over the lack of control over her personal data, the inability to curtail certain uses of the data, and the consequences of the Data Breach. The harm Plaintiff's suffered can be redressed by a favorable decision in this matter.

29. Plaintiff faces a substantial risk of future smishing (SMS message), vishing (voice messaging) or other social engineering-based attacks where full names, addresses, and phone numbers were stolen by a cybercriminal. Names, telephone numbers, and/or email addresses can be used by cybercriminals to launch social engineering attacks designed to trick individuals into giving away sensitive information. Defendant's credit identity monitoring, insurance, and restoration services do not protect Plaintiff from these types of attacks.

30. If Plaintiff and other Class Members (later defined) are tricked by a social engineering-based attack, criminals will be able to circumvent credit monitoring services.

Therefore, Plaintiff will incur out of pocket costs for purchasing products to protect from smishing (SMS message), vishing (voice messaging), pretexting, and other social engineering-based attacks.

31. Armed with the PII acquired in the Data Breach, data thieves have already engaged in theft and can, in the future, commit a variety of crimes including, opening new financial accounts, taking out loans, using Plaintiff's information to obtain government benefits, file fraudulent tax returns, obtain driver's licenses, and give false information to police during an arrest.

32. As a result of the Data Breach, Plaintiff suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PHI/PII; (iii) lost or diminished value of PHI/PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) general damages; (ix) nominal damages; (x) loss of control over PHI/PII; and (xi) emotional distress from the continued and increased risk the PHI/PII will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access on the dark web or otherwise; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

33. Defendant represented that it would use reasonable technical, administrative, and physical safeguards to protect the PHI/PII in its custody. These representations were made in the applicable privacy policy, business associates agreements, and through other disclosures in compliance with statutory privacy requirements.

34. Plaintiff and the Class Members relied on Defendant's representations and on this sophisticated business entity to keep their PHI/PII confidential, securely maintained, and to make only authorized disclosures of this information.

35. Upon information and belief, the Data Breach was a direct result of Defendant's failure to: (i) identify risks and potential effects of collecting, maintaining, and sharing personal information; (ii) adhere to its published privacy practices; (iii) implement reasonable data protection measures for the collection, use, disclosure, and storage of PHI/PII; and/or (iv) ensure its third-party vendors were required to implement reasonable data protection measures consistent with Defendant's data protection obligations.

Data Breaches Are Avoidable

36. The Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), has issued guidance documents regarding compliance with the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, HHS has developed guidance and tools to assist HIPAA covered entities and business associates in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of PHI and comply with the risk analysis requirements of the Security Rule.[12]

37. To detect and prevent cyber-attacks, Defendant could and should have implemented administrative, physical, and technical safeguards including, but not limited to, the following:

Administrative Safeguards

a. Implement policies and procedures to prevent, detect, contain, and correct security violations.

[12] *See*, U.S. Department of Health & Human Services, Security Rule Guidance Material, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

b. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the Defendant.

c. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

d. Apply appropriate sanctions against employees who fail to comply with the Defendant's security policies and procedures.

e. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

f. Identify a security official who is responsible for the development and implementation of the Defendant's policies and procedures to prevent, detect, contain, and correct security violations.

g. Implement procedures: (i) for the authorization and/or supervision of employees who work with electronic protected health information or in locations where it might be accessed; (ii) to determine whether an employee's access to electronic protected health information is appropriate; and (iii) for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends.

h. Implement policies and procedures that, based upon the Defendant's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

i. Implement a security awareness and training program for all members of Defendant's workforce, including procedures for guarding against, detecting, and reporting malicious software.

j. Implement policies and procedures to address how the Defendant will identify and respond to suspected or known security incidents; mitigate, to the extent practicable, known harmful effects of security incidents; and document security incidents and their outcomes.

k. Establish, (and implement as needed), policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information.

l. Perform a periodic technical and nontechnical evaluation in response to environmental or operational changes affecting the security of electronic protected health information.

m. Contractually obtain satisfactory assurances that business associates will appropriately safeguard electronic protected health information.

n. Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities.

o. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate.

p. Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information.

Physical Safeguards

q. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

r. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

s. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

Technical Safeguards

t. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

u. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

v. Implement a mechanism to encrypt and decrypt electronic protected health information.

w. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

x. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

y. Regularly patch critical vulnerabilities in operating systems, software, and firmware on devices. Consider using a centralized patch management system.

z. Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems.

aa. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.

bb. Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems.

cc. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email.

dd. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

ee. Configure firewalls to block access to known malicious IP addresses.

ff. Set anti-virus and anti-malware programs to conduct regular scans automatically.

gg. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

hh. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

ii. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

jj. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

kk. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

ll. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

mm. Execute operating system environments or specific programs in a virtualized environment.

nn. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

oo. Conduct an annual penetration test and vulnerability assessment.

pp. Secure your backups.[13]

qq. Identify the computers or servers where sensitive personal information is stored.

rr. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

[13] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (accessed June 11, 2024).

ss. Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

tt. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.

uu. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

vv. Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.

ww. To detect network breaches when they occur, consider using an intrusion detection system.

xx. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[14]

38. Given that Defendant collected, used, and stored PHI/PII, Defendant could and should have identified the risks and potential effects of collecting, maintaining, and sharing personal information.

39. Without identifying the potential risks to the personal data in Defendant's possession, Defendant could not identify and implement the necessary measures to detect and prevent cyberattacks. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and the Class Members' PHI/PII.

40. Defendant knew and understood that unencrypted PHI/PII is valuable and highly sought after by cybercriminals seeking to illegally monetize that data. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PHI/PII

[14] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (accessed June 11, 2024).

and of the foreseeable consequences that would occur if a data breach occurred, including the significant cost that would be imposed on Plaintiff and the Class Members as a result.

Plaintiff and Class Members Sustained Damages in the Data Breach

41. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes an actual, particularized, redressable injury traceable to the Defendant's conduct. As a consequence of the Data Breach, Plaintiff and Class Members sustained monetary damages that exceed the sum or value of $5,000,000.00.

42. Additionally, Plaintiff and Class Members face a substantial risk of future identity theft, fraud, or other exploitation where their names and social security numbers were targeted by a sophisticated hacker. The substantial risk of future identity theft and fraud created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

43. Furthermore, Plaintiff and Class Members face a substantial risk of future phishing, pretexting, or other attacks designed to trick them into sharing sensitive data, downloading malware, or otherwise exposing themselves to cybercrime, where their names and contact information were acquired in the Data Breach and potentially released on the dark web. The substantial risk of future exploitation created by the Data Breach constitutes a redressable injury traceable to the Defendant's conduct.

44. Upon information and belief, a criminal can easily link data acquired in the Data Breach with information available from other sources to commit a variety of fraud related crimes. An example of criminals piecing together bits and pieces of data is the development of "Fullz" packages.[15] With "Fullz" packages, cyber-criminals can combine multiple sources of PII to apply for credit cards, loans, assume identities, or take over accounts.

[15] "Fullz" is term used by cybercriminals to describe "a package of all the personal and financial records that thieves would need to fraudulently open up new lines of credit in a person's name." A Fullz package typically includes the

45. Given the type of targeted attack in this case, the sophistication of the criminal responsible for the Data Breach (it took Defendant three months to understand how the breach occurred), the categories of data involved in the Data Breach, hackers' typical behavior in other data breaches, the ability of criminals to link data acquired in the Data Breach with information available from other sources, and the fact that the stolen information has been placed, or will be placed, on the dark web, it is reasonable for Plaintiff and the Class Members to assume that their PHI/PII was obtained by, or released to, criminals intending to utilize the data for future identity theft-related crimes or exploitation attempts.

46. The substantial risk of future identity theft, fraud, or other exploitation that Plaintiff and Class Members face is sufficiently concrete, particularized, and imminent that it necessitates the present expenditure of funds to mitigate the risk. Consequently, Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach.

47. For example, the Federal Trade Commission has recommended steps that data breach victims take to protect themselves and their children after a data breach, including: (i) contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity); (ii) regularly obtaining and reviewing their credit reports; (iii) removing fraudulent charges from their accounts; (iv) closing new accounts opened in their name; (v) placing a credit freeze on their credit; (vi) replacing government-issued identification; (vii) reporting misused Social Security numbers; (viii) contacting utilities to ensure

victim's name, address, credit card information, social security number, date of birth, bank name, routing number, bank account numbers and more. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm

no one obtained cable, electric, water, or other similar services in their name; and (ix) correcting their credit reports.[16]

48. As a consequence of the Data Breach, Plaintiff and Class Members sustained or will incur monetary damages to mitigate the effects of an imminent risk of future injury. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year. The cost of dark web scanning and monitoring services can cost around $180 per year. The cost of spam and scam blockers can be about $60.00 a year per phone line.

49. As a result of the Data Breach, Plaintiff's and Class Members' PHI/PII, which has an inherent market value in both legitimate and illegitimate markets, has been damaged and diminished by its unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PHI/PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

50. Personal information is of great value, in 2019, the data brokering industry was worth roughly $200 billion.[17] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[18] Sensitive PII can sell for as much as $363 per record.[19] Further, a stolen medical identity has a $50 value on the black market.[20]

---

[16] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

[17] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[18] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[19] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[20] Study: Few Aware of Medical Identity Theft Risk, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm

51. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. By transacting business with Plaintiff and Class Members, collecting their PHI/PII, and then permitting the unauthorized disclosure of the information, Plaintiff and Class Members were deprived of the benefit of their bargain.

52. When agreeing to pay Defendant for products or services, consumers understood and expected that they were, in part, paying for the protection of their personal data, when in fact, Defendant did not invest the funds into implementing reasonable data security practices. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

53. Plaintiff brings this class action lawsuit individually, and on behalf of all those similarly situated, to address Defendant's inadequate data protection practices and for failing to provide timely and adequate notice of the Data Breach. Plaintiff has a continuing interest in ensuring that personal information is kept confidential and protected from disclosure, and Plaintiff should be entitled to injunctive and other equitable relief.

JURISDICTION & VENUE

54. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C.§1332, because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from each Defendant.

55. This Court has personal jurisdiction over Defendant because its principal place of business is in this District. Defendant has also purposefully availed itself of the laws, rights, and benefits of the State of Utah.

56. Venue is proper under 28 U.S.C §1391(b) because Defendant maintains a principal place of business in this District and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

PARTIES

57. Plaintiff Sierra Vent is a citizen of the State of South Carolina. At all relevant times, Plaintiff has been a resident of Darlington, Darlington County, South Carolina. Plaintiff purchased a health plan for which Defendant was the directed third-party administrator. The invasion of Plaintiff's privacy, the loss of control over her personal data, and the potential consequences of the Data Breach has caused Plaintiff emotional distress.

58. Defendant, HealthEquity Inc., is a corporation formed under the laws of Delaware, and maintains a principal place of business at 15 West Scenic Pointe Drive, Suite 100, Draper, Salt Lake County, Utah 84020. Defendant's registered agent for service of process is CT Corporation System, 1108 E. South Union Avenue, Midvale, Utah 84047.

CLASS ALLEGATIONS

59. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

60. The Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class**: All individuals residing in the United States whose PHI/PII was accessed and acquired by an unauthorized party as a result of a data breach that occurred on, or about, March 25, 2024, as reported by Defendant (the "Class").
>
> **South Carolina Subclass**: All individuals residing in South Carolina whose PHI/PII was accessed and acquired by an unauthorized party as a result of the data breach that occurred on, or about, March 25, 2024, as reported by Defendant (the "South Carolina Subclass").
>
> **Health Benefits Subclass**: All individuals residing in the United States who chose to continue group health benefits through a Consolidated Omnibus Budget Reconciliation Act (COBRA)

health plan for which Defendant was the directed third-party administrator and whose PHI/PII was accessed and acquired by an unauthorized party as a result of the data breach that occurred on, or about, March 25, 2024, as reported by Defendant (the "Health Benefits Subclass").

61. Collectively, the Class, Health Benefits Subclass, and South Carolina Subclass are referred to as the "Classes" or "Class Members."

62. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

63. Plaintiff reserves the right to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

64. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief, 4.3 million individuals were impacted in Data Breach.

65. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

66. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect

to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

67. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

68. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit many Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

69. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited

resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

70. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

71. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. The questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, includes the following:

a. Whether and to what extent Defendant had a duty to protect the PHI/PII of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PHI/PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant failed to adequately safeguard the PHI/PII of Plaintiff and Class Members;

d. Whether Defendant required its third-party vendors to adequately safeguard the PHI/PII of Plaintiff and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI/PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PHI/PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the practices, procedures, or vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach.

72. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

73. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PHI/PII of the Classes, and Defendant may continue to act unlawfully as set forth in this Complaint.

74. Further, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

75. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the Classes of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PHI/PII;

c. Whether Defendant's (or their vendors') security measures to protect its network were reasonable in light of industry best practices;

d. Whether Defendant's (or their vendors') failure to institute adequate data protection measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PHI/PII;

f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of personal information; and

g. Whether adherence to HIPAA rules and/or other data privacy recommendations and best practices would have prevented the Data Breach.

CAUSES OF ACTION
(*On behalf of Plaintiff and the Classes*)

COUNT 1: NEGLIGENCE/NEGLIGENCE *PER SE*

76. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

77. Defendant collects, creates, or shares information about Plaintiff's and Class Members' health status, provision of health care, or payment for health care that can be used to identify Plaintiff and Class Members.

78. Defendant had full knowledge of the types of unencrypted, electronically stored PHI/PII in its custody, the risks to the confidentiality and security of that information, and the types of harm that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

79. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PHI/PII, Defendant assumed a duty to use reasonable means to safeguard the personal data it obtained.

80. Defendant's duty included a responsibility to ensure it: (i) implemented reasonable administrative, technical, and physical measures to detect and prevent unauthorized intrusions into its information technology system and cloud environments; (ii) contractually obligated its vendors

to adhere to the requirements of Defendant's privacy policy; (iii) complied with applicable statutes and data protection obligations; (iv) conducted regular privacy assessments and security audits of its vendors' data processing activities; (v) regularly audited for compliance with contractual and other applicable data protection obligations; and, (vi) provided timely notice to individuals impacted by a data breach event.

81. Defendant is a business associate, as defined by HIPAA and, under the HITECH Act of 2009, is required to comply with the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A, C, and E. Under these rules, Defendant had a duty to implement reasonable and appropriate safeguards for the protected health information under its control.

82. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notification no later than 60 calendar days after the discovery of an unauthorized disclosure of unencrypted protected health information.

83. The Data Breach occurred on March 25, 2024, but Defendant did not provide Plaintiff and the Classes with notice of the event until roughly five months after the event.[21] Assuming, without conceding, that Defendant did not "discover" the "unauthorized access to and disclosure of protected health information and/or personally identifiable information stored in an unstructured data repository" until June 10, 2024, Defendant did not provide notice until August 26, 2024.

[21] The Notice of Data Breach letter was dated August 23, 2024. Assuming the notice was mailed on August 23, 2024, and presuming the letter was received three days after it was mailed, then Plaintiff and Class Members were provided notice of the breach on August 26, 2024.

84. Defendant had a duty to notify Plaintiff and the Classes of the Data Breach promptly and adequately. Such notice was necessary to allow Plaintiff and the Classes to take steps to investigate, prevent, mitigate, and repair any fraudulent usage of their PII.

85. Additionally, Defendant breached its duties under HIPAA by failing to conduct regular privacy assessments and security audits; failing to implement reasonable safeguards; and/or failing to continuously monitor its vendors' security practices and/or continuously monitor its vendors for data exposures and compromised credentials.

86. Defendant's violations of HIPAA Privacy, Security and Breach Notice Rules, constitutes negligence *per se* because these laws were designed specifically to protect the Plaintiff and Class Members from the unauthorized disclosure of their PHI/PII and the type of harm that resulted from the Data Breach was the type of harm the statue was intended to guard against.

87. Defendant also had a duty under its published privacy policy. Defendant's published privacy policy provides, in part, "We maintain administrative, technical, and physical safeguards designed to protect the information that you provide on this website and in connection with the Services from unauthorized access to or acquisition of such information . . . . [HealthEquity will require] our subcontractors to maintain the same privacy and security standards for protecting your information as we do."

88. One of Defendant's "Guiding Principles" for securing the PHI/PII in its custody is the Zero Trust Model, which requires strict access controls to reduce the possibility of unauthorized access and data breaches. A key component of the Zero Trust framework is multi-factor authentication (MFA), which requires multiple forms of verification before granting access to resources, such as cloud storage. MFA reduces the risk of data breaches by requiring more than

just a username and password—a security token or biometric factor for example—to access resources.

89. Defendant breached its duty by failing to require its subcontractors/business partners to implement MFA before permitting access to cloud resources. The Data Breach occurred because one of Defendant's vendors—with access to the cloud storage environment—had their account credentials compromised. Had Defendant adhered to its own privacy policy regarding the confidentiality and security of Plaintiff's and Class Members' information, the Data Breach could have been prevented.

90. Defendant breached its duties under the privacy policy, and thus was negligent. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to encrypt PHI/PII in transit and at rest.

b. Failing to adopt, implement, and maintain reasonable administrative, technical, and physical measures to safeguard PHI/PII.

c. Failing to adequately assess the privacy and security risks created by vendors with access to Defendant's networks, systems and resources.

d. Allowing unauthorized access to PHI/PII.

e. Failing to detect in a timely manner that PHI/PII had been compromised.

f. Failing to destroy or delete PHI/PII it was no longer required to retain.

g. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

h. Failing to implement data security practices consistent with Defendant's published privacy policies, industry standards and compliance obligations.

91. The injuries resulting to Plaintiff and the Classes because of Defendant's failure to use adequate security measures was reasonably foreseeable.

92. Plaintiff and the Classes were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing PHI/PII and the critical importance of protecting that data.

93. Plaintiff and the Classes had no ability to protect the PHI/PII in Defendant's possession. Defendant was in the best position to protect against the harms suffered by Plaintiff and the Classes as a result of the Data Breach.

94. But for Defendant's breach of duties owed to Plaintiff and the Classes, their PHI/PII would not have been compromised. There is a close causal connection between Defendant's failure to implement reasonable security measures to protect the PHI/PII of Plaintiff and the Classes and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

95. As a result of the Data Breach, Plaintiff and the Classes suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PHI/PII; (iii) lost or diminished value of PHI/PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) general damages; (ix) nominal damages; (x) loss of control over PHI/PII; and (xi) emotional distress from the continued and increased risk the PHI/PII will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access on the dark web or otherwise; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

96. Plaintiff and Class Members are entitled to compensatory and consequential damages sustained as a result of the Data Breach, including, but not limited to, the cost of future credit monitoring, scam call/text blockers, and dark web monitoring services.

97. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) regularly assess the risks to its entire attack surface and confirm that its administrative, technical, and physical safeguards are appropriate to protect the PHI/PII in its custody; (ii) continuously monitor its vendors, at least once per year, to identify potential ways a threat actor could gain access to PHI/PII or other confidential information; and (iii) implement an administrative process for regularly auditing its subcontractors' privacy and security standards, including, adherence to a Zero Trust model of strict access controls to reduce the possibility of unauthorized disclosures of PHI/PII; and (iv) comply with the HIPAA Privacy, Security and Breach Notice Rules.

COUNT 2: BREACH OF IMPLIED CONTRACT

98. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

99. Defendant creates or collects PHI/PII in the ordinary course of providing its services.

100. Defendant published a privacy policy to inform the public about how Defendant collects, uses, shares, and protects the information Defendant gathers in connection with the provision of those products or services. Defendant's published privacy policy provides, in part, "We maintain administrative, technical, and physical safeguards designed to protect the information that you provide on this website and in connection with the Services from unauthorized access to or acquisition of such information . . . . [HealthEquity will require] our subcontractors to maintain the same privacy and security standards for protecting your information as we do."

101. In so doing, Plaintiff and Class Members entered implied contracts with Defendant by which Defendant agreed to: (i) use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information it collects and stores; and (ii) require its subcontractors to maintain same privacy and security standards.

102. Defendant would not have been granted access to Plaintiff's and the Classes PHI/PII in the absence of an expressed or implied promise to implement reasonable data protection measures.

103. Plaintiff and Class Members fully and adequately performed their obligations under the implied contract with Defendant. Plaintiff and Class Members had no bargaining power in the transaction and were obligated to consent to the disclosure of their PII/PHI to the Defendant since Defendant was the third-party administrator for a group health benefit plan associated with the Plaintiff and Class Members.

104. Defendant breached the implied contract with Plaintiff and Class Members which arose from the course of conduct between the parties, as well as disclosures on the Defendant's web site (https://www.healthequity.com), privacy policy, and in other documents, all of which created a reasonable expectation that the personal information Defendant collected would be adequately protected and that the Defendant would take such actions as were necessary to prevent unauthorized access to and disclosure of such information.

105. As a direct and proximate result of the Defendant's breach of an implied contract, Plaintiff and the Classes suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PHI/PII; (iii) lost or diminished value of PHI/PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of

benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) general damages; (ix) nominal damages; (x) loss of control over PHI/PII; and (xi) emotional distress from the continued and increased risk the PHI/PII will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access on the dark web or otherwise; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

106. Plaintiff and Class Members are entitled to nominal, compensatory, and consequential damages sustained as a result of the Data Breach, including, but not limited to, the cost of future credit monitoring, scam call/text blockers, and dark web monitoring services.

107. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) regularly assess the risks to its entire attack surface and confirm that its administrative, technical, and physical safeguards are appropriate to protect the PHI/PII in its custody; (ii) continuously monitor its vendors, at least once per year, to identify potential ways a threat actor could gain access to PHI/PII or other confidential information; and (iii) implement an administrative process for regularly auditing its subcontractors' privacy and security standards, including, adherence to Defendant's Zero Trust model of strict access controls to reduce the possibility of unauthorized disclosures of PHI/PII; and (iv) comply with the HIPAA Privacy, Security and Breach Notice Rules.

COUNT 3: UNJUST ENRICHMENT

108. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

109. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

110. Defendant obtained the Plaintiff's and Class Members' PHI/PII as part of the administration of a health insurance plan, which conferred a monetary benefit on Defendant. Defendant knew that this monetary benefit was being conferred and has accepted and retained that benefit.

111. By collecting the PHI/PII, Defendant was obligated to safeguard and protect such information, to keep such information confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been compromised or stolen.

112. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, it would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members conferred upon Defendant without paying value in return.

113. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) regularly assess the risks to its entire attack surface and confirm that its administrative, technical, and physical safeguards are appropriate to protect the PHI/PII in its custody; (ii) continuously monitor its vendors, at least once per year, to identify potential ways a threat actor could gain access to PHI/PII or other confidential information; and (iii) implement an administrative process for regularly auditing its subcontractors' privacy and security standards, including, adherence to a Zero Trust model of strict access controls to reduce the possibility of unauthorized disclosures of PHI/PII; and (iv) comply with the HIPAA Privacy, Security and Breach Notice Rules.

114. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

COUNT 4: INVASION OF PRIVACY

115. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

116. Plaintiff and Class Members had a legitimate expectation of privacy in their protected health information and other personally identifying information such as their social security numbers, health card numbers, health plan member numbers, diagnoses, prescription details, and payment card information. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

117. Defendant owed a duty to Plaintiff and Class Members to keep their PHI/PII confidential.

118. Defendant permitted the public disclosure of Plaintiff's and Class Members' PHI/PII to unauthorized third parties.

119. The PHI/PII that was disclosed without the Plaintiff's and Class Members' authorization was highly sensitive, private, and confidential. The public disclosure of the type of PHI/PII at issue here would be highly offensive to a reasonable person of ordinary sensibilities and was offensive to the Plaintiff and Class Members.

120. Defendant permitted its vendors to maintain an information technology environment that was vulnerable to foreseeable threats, which created an atmosphere for the Data Breach to occur. Despite knowledge of the substantial risk of harm (or failing to identify the

substantial risk of harm) created by these conditions, Defendant intentionally disregarded the risk, thus permitting the Data Breach to occur.

121. By permitting the unauthorized disclosure, Defendant acted with reckless disregard for the Plaintiff's and Class Members' privacy, and with knowledge that such disclosure would be highly offensive to a reasonable person. Furthermore, the disclosure of the PHI/PII at issue was not newsworthy or of any service to the public interest.

122. Defendant was aware of the potential of a data breach and failed to implement appropriate policies and procedures to prevent the unauthorized disclosure of Plaintiff's and Class Members' data.

123. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PHI/PII to rise to the level of intentionally allowing the intrusion upon the seclusion, private affairs, or concerns of Plaintiff and Class Members.

124. Plaintiff and Class Members have been harmed by the invasion of their privacy, have lost control over their personal information, and have sustained damages in an amount to be determined at trial.

COUNT 5: VIOLATION OF THE SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT {S.C. Code. Ann. §§39-5-10 *et seq*.}

125. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

126. Defendant obtained the Plaintiff's and Class Members' PHI/PII as part of the administration of a health insurance plan.

127. Defendant gathered and stored the PII/PHI of Plaintiff and Class Members as part of its business. Plaintiff and Class Members entrusted Defendant with their PII/PHI with the

understanding that Defendant would adequately safeguard their information.

128. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices include failing to adhere to a company's published privacy policies. Such behavior by Defendant also constitutes a false, misleading, or deceptive act under the South Carolina Unfair Trade Practices Act ("SCUTPA"). *See*, S.C. Code Ann. §39-5-20(b).

129. Defendant violated the state consumer protection statute by failing to adhere to its own privacy policy regarding the confidentiality and security of Plaintiff's and Class Members' information. More specifically, Defendant violated the SCUTPA by failing to require its vendors to maintain the same privacy and security standards as the Defendant, including, implementing a Zero Trust Model of strict access controls to reduce the possibility of unauthorized access to PHI/PII. Defendant further violated the state consumer protection statute by failing to use reasonable administrative, technical, or physical measures to protect PHI/PII as is represented in its privacy policy.

130. Defendant's conduct created a likelihood of confusion, deception, or misunderstanding regarding its actual data privacy and security practices. Defendant promised to protect Plaintiff's and Class Members' PII/PHI via its privacy policies, but allowed the unauthorized access to this personal and protected health information; Defendant failed to disclose material facts that the Plaintiff's and Class Members' PII/PHI would be disclosed to unauthorized third parties; Defendant failed to obtain Plaintiff's and Class Members' consent in transmitting their PII/PHI to a third party; and Defendant knowingly violated industry and legal standards regarding the protection of Plaintiff's and Class Members' PII/PHI.

131. Defendant's unfair or deceptive acts affected public interests, including those of

Plaintiff and Class Members. Defendant knew or should have known that it was likely to mislead its customers who were acting reasonably. Defendant engaged in unfair or deceptive practices by breaching its duties to provide technical and administrative data security policies, procedures, and practices, including vendor risk assessment and mitigation. Defendant's failure to adhere to its published privacy policies and procedures is offensive to established public policy and is substantially injurious to consumers as evidenced by the massive Data Breach.

132. Plaintiff and Class Members had no idea or indication that Defendant would not follow its own published privacy practices, and they had no choice in the selection of Defendant's services. Defendant's deceptive acts, as described herein, proximately caused Plaintiff and Class Members damages.

133. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered damages including, but not limited to: (i) invasion of privacy; (ii) theft of PHI/PII; (iii) lost or diminished value of PHI/PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) statutory damages; (viii) general damages; (ix) nominal damages; (x) loss of control over PHI/PII; (xi) attorney's fees and expenses; and (xii) emotional distress from the continued and increased risk the PHI/PII will be further misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access on the dark web or otherwise; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the data.

134. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their PHI/PII and remain

at imminent risk that further compromises of their PHI/PII will occur in the future, as a result of Defendant's deceptive trade practices. As such, the remedies available at law are inadequate to compensate for that injury. Accordingly, Plaintiff and Class Members also seek to obtain a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure PHI/PII and to timely notify consumers of a data breach under the common law, HIPAA, Section 5 of the FTC Act, SCUTPA, and various state statutes.

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff and Class Members' PHI/PII.

135. The Court should also issue corresponding prospective injunctive relief requiring that Defendant employs adequate data protection practices consistent with law and industry standards.

136. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff will likely be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

137. The issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by encouraging Defendant to take necessary action to prevent another data breach, thus eliminating the additional injuries that would result to Plaintiff and the multitude of individuals whose PII would be at risk of future unauthorized disclosures.

138. As a result of the Defendant's false, misleading, or deceptive acts, regarding its data security practices, the consuming public in general, Plaintiff, and Class Members suffered

injuries including, but not limited to, the future and continued risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

139. Plaintiff and Class Members are entitled to attorneys' fees, costs, and injunctive relief requiring Defendant to: Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) regularly assess the risks to its entire attack surface and confirm that its administrative, technical, and physical safeguards are appropriate to protect the PHI/PII in its custody; (ii) continuously monitor its vendors, at least once per year, to identify potential ways a threat actor could gain access to PHI/PII or other confidential information; (iii) implement an administrative process for regularly auditing its subcontractors' privacy and security standards, including, adherence to a Zero Trust model of strict access controls to reduce the possibility of unauthorized disclosures of PHI/PII; (iv) comply with the HIPAA Privacy, Security and Breach Notice Rules; (v) implement strong authentication mechanisms for accessing cloud services; and (vi) provide adequate dark web monitoring and fraud protection to all affected by the Data Breach.

140. Plaintiff brings this action to protect the citizens of South Carolina from unfair or deceptive acts in the conduct of any trade or commerce

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully requests that the Court enter judgment as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Classes and counsel for Plaintiff(s) as Class Counsel;

B. For an order declaring the Defendant's conduct violates the statues and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

D. Ordering Defendant to pay for lifetime credit monitoring and dark web scanning services for Plaintiff and the Classes;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;

H. For injunctive relief as pleaded or as the Court may deem proper; and

I. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated September 17, 2024

VALERGA LLP

/s/Brody Valerga
Brody Valerga

-AND-

POULIN | WILLEY | ANASTOPOULO

/s/Paul J. Doolittle
Paul J. Doolittle, Esq.*
Attorneys for Plaintiff

**Pro Hac Vice forthcoming*